

Amendments to the Specification:

Please replace the paragraphs starting on page 8, line 20, through page 9, line 25, with the following amended paragraphs, which correct for typographical errors:

According to the present invention, the remote unit 30 is implemented for repetitively transmitting an identification signal that is recognized by the base unit [[11]]12 when the remote unit 30 is not more than a predetermined distance from the base unit [[11]]12. Typically, the predetermined distance is a distance beyond which the identification signal is not recognizable by the base unit. Similarly, the base unit [[11]]12 repetitively transmits a trigger signal that is recognizable by the remote unit 30 when the remote unit is within the predetermined distance from the base unit. When this bidirectional communication is interrupted in the case of the remote unit being transported out of range, alarms are activated in both the base unit [[11]]12 and the remote unit 30 in one embodiment. In a preferred exemplary configuration of the system 10, transmission of the identification signal from the remote unit is in response to a periodic trigger signal from the base unit, the form of the trigger signal being dependent on whether the identification signal is being recognized at the base unit [[11]]12. For example, a test bit of the trigger signal can be toggled on or off depending on whether the identification signal is properly received. The toggling can be to alternate states in each cycle for facilitating verification of valid communication based on changed states of the test bit. The test bit can then be reflected back to the base unit as an element of the identification signal for base unit verification of bidirectional communication.

The remote unit 30 is also implemented for transmitting signature data such as pen position coordinate data to the base unit [[11]]12 in a suitable manner as described, for example, in the above-referenced '955 patent. The remote computer 32 and/or the signature tablet 34 preferably has suitable memory associated therewith for temporarily storing signature data, at least during intervals of time that the remote unit 30 is out of range from the base unit 12. Transceivers suitable for use as the base

transceiver 22 and the remote transceiver ~~[[39]]38~~ are available as Part No. AC5124C from Aerocomm of Lenexa, KS.

In the exemplary configuration shown in Fig. 1, the remote unit 30 is installed with the signature tablet ~~[[33]]34~~ in a transportable canister 40 that is configured for use in the transaction facility 11, the facility 11 also including a vacuum transport tube 41 and, optionally, a main computer 42, the main computer ~~[[44]]42~~ preferably having a communication link 43 to the base computer 13. The canister 40 has a conventional door 44 that opens an interior compartment 45, the compartment being used for carrying documents between users (typically customers) and the transaction facility 11, and for storing the stylus 36. Preferably the compartment 15 and the stylus 16 have complementary elements 46A and 46B of a retainer such as a hook-loop fastener affixed thereto for releasably capturing the stylus 36 when it is not in use. Preferably the canister ~~[[42]]40~~ incorporates a door sensor 48 for signaling whether the door 44 is open or closed.

Please replace the paragraph on page 10, lines 9 through 30, with the following amended paragraph, which corrects for typographical errors:

An additional preferred feature of the remote unit 30 is a docking connector 56 for use with a docking device 26 in communication with the base unit 12 to enable wired or local communication of data between the remote unit 30 and the base unit 12 when the remote unit is docked relative to the transaction facility 11 as indicated by broken lines in Fig. 1. This arrangement allows the signature data to be transmitted to the base computer 13 using the transceivers 22 and ~~[[39]]38~~, or using a communication link 27 between the docking device and the base device interface 20, depending on circumstances such as the performance of the transceivers 22 and ~~[[39]]38~~, and the need, if any, to provide the signature data to the base unit 12 prior to return of the canister 40 to the transaction facility 11. It will also be understood that the communication link 27 can be the exclusive channel for communicating the signature data, such that the transceivers 22 and ~~[[39]]38~~ can be low cost devices that may not be

capable of quickly communicating the signature data. Further, the communication link can be a wired connection or, optionally, it can include a radio transmitter and receiver, or it can utilize infrared technology, depending on factors such as the distance and obstacles between the docking device and the base device interface. In another variation, separate counterparts of the base and remote transceivers 22 and ~~[[39]]~~38 can be used for transmitting the signature data and for monitoring the proximity of the canister 40 with the transaction facility. In this variation, the transceivers monitoring proximity would have an effective range commensurate with appropriate distances that users might be authorized to transport the canister 40, but would need only low bandwidth capability. The transceivers used for signature data transfer would need higher bandwidth capability, but could operate at short range with the canister in close proximity to the transaction facility 11.

Please replace the paragraph on page 11, lines 10 through 23, with the following amended paragraph, which corrects for a typographical error:

The base voice interface and the remote voice interface 39 each include a digital to analog converter (DAC) and an analog to digital converter (ADC). Voice from the base unit 12 is picked up by the base microphone 19 and routed through a PC sound card or other suitable mechanism for reproducing sound of the base computer 13 (such as by a microphone and pre-amp of the transaction facility 11) and fed through the ADC of the base voice interface 24 to the base transceiver 22. Then from the remote transceiver 38, received digital voice signals are fed into the remote voice interface 39 which signals the presence of the digital voice signal to the remote computer 32 which then activates the DAC of the remote voice interface to produce a reconstituted analog voice waveform that is amplified in the remote device interface 33 and delivered to the remote speaker 52. For voice from the remote unit 30 to the base unit 12, this process is reversed. It will be understood that the operator interface 14 can include a subset only of the above-described components thereof. Also, either or both of the device interfaces 20

and 33 can be integrated with the respective computers ~~[[12]]~~13 and 32.

Please replace the paragraph starting on page 12, line 23, through page 13, line 7, with the following amended paragraph, which corrects for a typographical error:

In the standby mode, after a wait interval of perhaps 15 seconds, the remote transceiver 38 is powered (momentarily) for verifying continued communication with the base unit ~~[[13]]~~12, in a counterpart of the test communication step 64. If so, the standby mode maintained, control passing to the counterpart test door open step 62, further described below, the standby mode providing greatly reduced power consumption by the remote unit 30. If the counterpart test communication step 64 produces a negative result during the standby mode, the remote transceiver 38 is cycled off then on again in an interrupt transceiver step 68, and reestablishment of communication is determined in a test reconnect step 69. If not, the recycling of the remote transceiver is repeated up to two more times. If the communication is not reestablished within three cycles, the alarm is turned on, the remote unit 30 remaining in standby mode as long as the door 44 remains closed, the remote transceiver again being turned off for the wait interval, after which the counterpart test communication step 64 is repeated. In accordance with the above description, the verification of communication by the remote unit 30 can include testing whether the trigger signals are being received from the base unit 12, and further verifying that the trigger signals are characteristic of the identification signals being properly received from the remote unit by the base unit.

Please replace the paragraphs starting on page 13, line 23, through page 14, line 19, with the following amended paragraphs, which correct for typographical errors and a grammatical error:

When the door 44 is opened during the standby mode, control is returned to the transceiver on step 63, described above, and the process for obtaining another signature is repeated as described above. However, when the result of the test communication step 64 (prior to the ready signature step 65) is negative, the remote

LED is turned off (if powered) and the alarm is activated, control passing to a counterpart of the test door closed step 66. If the door 44 remains open, control passes to a counterpart of the test reconnect step 69, the alarm remaining activated while the counterpart steps 66 and 69 are repeated. If the door is closed while the alarm is on, the remote unit is placed in the standby mode for monitoring possible reestablishment of communication with the base unit [[13]]12. If communication is reestablished before the door 44 is closed, the alarm is deactivated and control is passed (or returned) to the ready signature step 65. Thus the remote unit 30 provides for capturing the user's signature 35 while communication with the base unit [[13]]12 is maintained, activating the alarm when communication is interrupted, and deactivating the alarm when communication is restored, using the standby condition to conserve transceiver power when the door 44 is closed, and when the alarm is activated.

With particular reference to Figs. 3 and 4, a base computer process 70 with which the base computer is programmed includes, following application of power, an initialize step 72 is performed in which the base indicator 25 is activated and a base alarm timer is set and activated. Then a determination of whether signature management software of the signature system has been started (ready to accept a signature) is performed in a test ready step 74. Typically, the signature management software, which can implement features described in the above-referenced '955 patent, is started by mouse-clicking on a start button being displayed on the screen display 15. This step makes the base unit ready to accept a signature whether or not the remote unit is ready to accept one. If the software is not started, the base indicator is deactivated and an alarm service routine 76 is invoked in a call alarm step 77. (The service routine 76 is shown as a subroutine for convenience, in that separate portions of the process 70 ~~incorporates~~incorporate the same steps.)

Please replace the paragraphs starting on page 15, line 25, through page 16, line 27, with the following amended paragraphs, which correct for typographical errors:

As described above, the base alarm timer has an exemplary timeout interval of 45 seconds. This is consistent with the standby mode of the remote unit 30 in which the remote transceiver ~~[[39]]~~38 is activated at intervals of 15 seconds for from approximately 0.25 second to approximately 1.5 seconds to verify communication with the base unit 12. The 15 second intervals advantageously facilitates providing battery power to permit effective use of the remote unit 30 for at least one day, while also limiting the distance that the remote unit could be taken away from effective communications range before the alarm would be activated. An additional consideration is that the metal used in typical implementations of the transport tube 41 acts as a shield to prevent communication with the base unit 12 for perhaps 15 seconds. Consequently, it is preferred that there be no activation of either the base alarm circuit 23 or the remote alarm circuit 37 if there is no communication for the first 15 seconds. A further consideration is that if the base unit timer starts right after a communication, it will run for another 15 seconds before the next communication. The remote transceiver is activated at the 15 second interval; if it sees no communication, and this is verified in the three cycles of the test reconnect step 69 of the remote computer process of Fig. 2, up to an additional 1.5 seconds can elapse, a total of 19.5 seconds. Allowance is made for this sequence to be completed twice, taking nearly 40 seconds, and further allowance for the time of communication which can vary depending on distance. The above considerations assume that the canister 40 is not actually being used. If the door 44 is opened when the canister 40 is out of range, the remote alarm circuit 37 is activated within 2 or 3 seconds notwithstanding the 45 second delay in activation of the base alarm circuit 23. This is because the remote computer process 60 executes the test communication step 64 substantially immediately following detection of initial opening of the door 44 at the test door open step 62 following power-up. If the canister 40 is out of range, the identification signals from the remote unit 30

are interrupted, and the trigger signals consequently are not toggled or otherwise characteristic of good communications between the base and remote units.

Thus the base unit 12 produces the trigger signals as a pulse train that is kept alive by reflection from the remote unit 30 back to the base unit, and both units activate respective alarms in response to interruption of the communication and also reset the alarms in response to restoration of communication. The base computer 13 can communicate with multiple remote units 30 using corresponding counterparts of the base device interface 20 and base transceiver 22, each pair of transceivers 22 and ~~[[39]]~~38 operating on frequencies (channels) different than those of other such pairs.

Please replace the paragraph starting on page 18, line 17, through page 19, line 5, with the following amended paragraph, which corrects for typographical errors:

When a stylus 125 is included in the compartment 120, it is preferably reversibly attached to an interior surface of the compartment 120. In the embodiments shown in Figures 5 and 8, the interior surface of the compartment 120 has attached thereto a first piece of hook-and-loop material 127 (such as Velcro brand hook-and-loop material, made by Velcro Industries B.V.) and the stylus 125 has attached thereto a corresponding second piece of hook-and-loop material 126 to which the first piece 127 becomes reversibly bound when brought into contact with the second piece 126. Other systems for reversibly binding the stylus 125 to the compartment can also be used. In an alternative embodiment (not shown), the compartment 120 further comprises a foam material which “pinches” or otherwise generally physically contacts and restrains the stylus 125 and thereby substantially prevents movement of the stylus ~~[[127]]~~125 when the transport housing 100 is in a closed position and is being moved. Means for preventing movement of the stylus ~~[[127]]~~125 are particularly important in embodiments in which the transport housing is moved rapidly, such as through a pneumatic tube, so that the stylus 125 does not impact the interior of the compartment 120 or the electronic signature tablet 140 or other device, thereby possibly damaging it. Such embodiments are also of more general applicability in maintaining a

stylus 125 within the compartment 120. It has been found to be disadvantageous to tether a stylus 125 to the compartment 120, such as via a cord, primarily for the reason that such a cord may get caught in the door 110 when it is closed and interfere with such closure, though the use of a retractable cord in the present invention is contemplated.

Please replace the paragraph on page 20, line 17 through line 24, with the following amended paragraph, which corrects for a typographical error:

The housing 100 can also further include a battery (not shown) for providing power to an attached or enclosed device, such as a device for capturing electronic data 140. The battery can be contained within a housing of the device itself, or alternatively can be contained in a battery housing 106. The battery housing 106 is preferably enclosed so as to protect it from environmental damage, such as from moisture, as well as from possible tampering by a user. In the embodiment shown in Figures 5, 6, 8 and 9, the battery housing 106 is accessible from the interior of the compartment 120 through a battery housing door 107 which is reversibly secured to an interior surface ~~[[121]]~~122 of the compartment 120, in this case by means of screws 108.